

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
BEAUMONT DIVISION

UNITED STATES OF AMERICA,

vs.

ALVARO ROMERO (1), and
SIDNEY ANTHONY WORRELL (10)

NO. 1:17-CR-00153-TH

REPORT AND RECOMMENDATION
GRANTING DEFENDANT'S MOTION TO SUPPRESS

Pending before the undersigned is a “Motion to Suppress Wiretap Evidence” filed by Defendants Alvaro Romero and Sidney Worrell (Doc. No. 172). Because the wiretap orders do not contain the identity of the high-level Justice Department official who approved the applications, the orders are facially insufficient. *See* 18 U.S.C § 2518(4)(d). Thus, the contents of the wire communications and evidence obtained therefrom should be suppressed pursuant to 18 U.S.C. § 2518(10)(a)(ii).

I. Background

In 2013 and 2014, the United States Drug Enforcement Administration investigated the Romero Drug Trafficking Organization. (Doc. No. 181 at 1.) During the investigation, the Government filed eight applications for orders authorizing the interception of wire and electronic communications (the “Wiretap Orders”) that are the subject of this Report and Recommendation.¹ Each Wiretap Order was presented to a district judge for the Southern District of Texas accompanied with an authorization letter signed by a Department of Justice official.

¹ (Doc. Nos. 181-1, p. 20; 181-2, p. 20; 181-3, p. 18; 181-4, p. 21; 181-5, p. 23; 181-6, p. 21; 181-7, p. 21; 181-8, p. 21.)

In December 2017, the Grand Jury sitting in the Eastern District of Texas returned a two-count Indictment alleging that Worrell, Romero, and their co-defendants violated 21 U.S.C. § 846 (Conspiracy to Possess with Intent to Distribute Cocaine HCL) and 18 U.S.C. § 1956(h) (Conspiracy to Launder Monetary Instruments). (Doc. No. 1.) On August 10, 2018, Worrell filed a Motion to Suppress Wiretap Evidence. (Doc. No. 172.) On September 6, 2018, United States District Judge Thad Heartfield referred Worrell's Motion to Suppress to the undersigned. (Doc. No. 190.)

On August 6, 2018, Romero pleaded guilty to Counts One and Two before United States Magistrate Judge Keith Giblin. (Doc. No. 163.) Before the district court accepted his guilty plea, Romero filed an Unopposed Motion to Adopt Worrell's Motion to Suppress and Unopposed Motion to Defer Acceptance of Guilty Plea. (Docs. 178 and 179, filed August 20, 2018.) On September 7, 2018 Romero's request to join in his co-defendant's motion to suppress was granted (Doc. No. 193), but his Motion to Defer Acceptance of Guilty Plea was not ruled on by the court.

On September 11, 2018, Judge Giblin issued a Report and Recommendation that the district court accept Romero's guilty plea. (Doc. No.195.) On September 26, 2018, Judge Heartfield adopted Judge Giblin's Recommendation and adjudged Romero guilty on Counts One and Two. (Doc. No. 196.) Romero then filed an Unopposed Motion to Vacate Judge Heartfield's order accepting his guilty plea which is currently pending. (Doc. No. 199, filed October 16, 2018.)

II. Title III Requirements

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90–351, 82 Stat. 197, 211–25 (codified as amended at 18 U.S.C. §§ 2510 *et seq.*) (“Title III”), sets forth a detailed procedure for the interception of wire, oral, or electronic communications. 18 U.S.C. § 2511; *cf. id.* §§ 2512–2513.

First, the wiretap application must be authorized by one of the statutorily identified high-level Justice Department officials, which specifically includes the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, or any acting Assistant Attorney General, as well as certain Deputy Assistant Attorneys General specially designated by the Attorney General. *See id.* § 2516(1).

Second, the government must submit the application, under oath or affirmation, to a judge of competent jurisdiction and affirm the authority to make such application. *Id.* § 2518(1). The application must contain certain information: (1) the identity of the officer(s) making and authorizing the application; (2) an explanation of the facts and circumstances that the applying officer believes justify the wiretap; (3) a statement describing the necessity of the wiretap to the government's investigation; (4) a statement of the period of time for which the interception is required to be maintained; (5) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application; and (6) if the application is for the extension of an order, a statement setting forth the results obtained thus far.² 18 U.S.C. § 2518(1)(a)–(f).

Third, before issuing the *ex parte* wiretap order, as requested or modified, a judge must make certain determinations based on the facts submitted by the applicant, *id.* § 2518(3), including, *inter alia*, that the wiretap is necessary to the investigation, *id.* § 2518(3)(c), and that there exists probable cause to believe that the phone to be tapped is or will soon be used in connection with particular enumerated criminal offenses, *id.* § 2518(3)(d).

² “The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.” *Id.* § 2518(2).

Fourth, the judge issues the order approving the wiretap. The court order must contain the following specific elements:

- (a) the identity of the person, if known, whose communications are to be intercepted;
- (b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;
- (c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;
- (d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and
- (e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

18 U.S.C. § 2518(4)(a)–(e) (hereinafter the “§ 2518(4) requirements”).

Title III also provides the means by which a Defendant can challenge the admissibility of wiretap evidence:

[a]ny aggrieved person in any trial, hearing, or proceeding in or before any court . . . may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that—

- (i) the communication was unlawfully intercepted;
- (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or
- (iii) the interception was not made in conformity with the order of authorization or approval.

18 U.S.C. § 2518(10)(a).

III. Standing and Scope

The Government first contests the Defendants’ standing to challenge the Wiretap Orders. As to Worrell, the Government claims that he was never intercepted over any of the phones tapped in the Wiretap Orders, and as to Romero, that he was neither a target subject nor intercepted under four of the eight orders.

A. Intercepted phone calls

Section 2518(10)(a) permits any “aggrieved person” to move to suppress the contents of wire or oral communications seized during electronic surveillance. 18 U.S.C. § 2518(10)(a). An aggrieved person is defined as “a person who was a party to any intercepted wire, oral or electronic communication or a person against whom the interception was directed.” *Id.* at 2518(11).

Worrell submitted an affidavit stating that he recognizes his voice on two of the eight telephone numbers: three phones calls from the 409-273-0566 phone number (authorized by the April 23, 2014 order) and seven phones calls related to the 832-727-2669 phone number (authorized by the May 14, 2014 order). (Doc. No. 194-1.) The Government has not challenged Worrell’s affidavit. Based upon Worrell’s uncontradicted affidavit, the undersigned finds that Worrell has standing to challenge the April 23 and May 14, 2014 orders pertaining to those numbers only.

The Government concedes that Romero was intercepted pursuant to orders issued on February 14, 2014³, March 21, 2014, April 23, 2014, and May 5, 2014. (Doc. No. 181, p. 2.) Romero has not filed an affidavit nor otherwise responded to the Government’s claim that he lacks standing to challenge the orders in which he was not intercepted. Accordingly, the undersigned finds that Romero’s standing is limited to only the orders listed above that authorized wiretaps in which he was actually intercepted.

³ The Government’s Response actually states that the February 21, 2014 order authorized an interception of a phone used by Romero. However, there is no February 21st order. Accordingly, the undersigned presumes the Government meant to refer to the February 14, 2014 order.

B. Suppression of text messages

The Government also claims that the scope of § 2518 does not allow for statutory suppression of electronic communications (*i.e.*, text messages) derived as a result of the Wiretap Orders. The Government claims that § 2518 only allows suppression of wire or oral communications, and that “[s]uppression for an order deemed facially insufficient is not available for intercepted electronic communications such as text messages.” (Doc. No. 181, p. 20.)

When first enacted, Title III addressed only the interception of wire and oral communications. Title III was amended in 1986 by the Electronic Communications Privacy Act (“ECPA”) of 1986, Pub. L. No. 99–508, 100 Stat. 1848 (1986), to expand certain protections previously only provided to wire and oral communications to now include electronic communications. *See, e.g.*, 18 U.S.C. § 2511(1)(a),(c), (d) and (e) (penalizing unauthorized interception of wire, oral and electronic communications). Electronic communications are defined as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.” 18 U.S.C. § 2510(12); *see United States v. Jones*, 451 F. Supp. 2d 71, 75 (D.D.C. 2006) (holding that text messages constitute “electronic communications”).

Section 2518(10)(a) provides that “[i]f the [suppression] motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter.” 18 U.S.C § 2518(10)(a)(iii). The Government claims that because § 2518(10)(a) does not also explicitly list “electronic communication,” suppression is not an available remedy for text messages. The Government argues that the

Defendants' only remedy to challenge electronic communications under § 2518 is to raise a Fourth Amendment-based objection.⁴

Many courts agree that the exclusionary rule of Title III does not apply to electronic communications. *See United States v. Apodaca*, 287 F. Supp. 3d 21, 31 (D.D.C. 2017) (holding that the exclusion remedy is limited to improper interception of wire and oral communications); *United States v. Steiger*, 318 F.3d 1039, 1052 (11th Cir. 2003) (examining the legislative history of the ECPA to conclude that “a statutory suppression remedy does not exist for unlawful interceptions of ‘electronic communications’”); *United States v. Meriwether*, 917 F.2d 955, 960 (6th Cir. 1990) (holding that “[t]he ECPA does not provide an independent statutory remedy of suppression for interceptions of electronic communications”); *United States v. Banks*, 2014 WL 4261344, at *2 (D. Kan. Aug. 29, 2014) (“the statutory suppression remedy extends to wire and oral communications only”). Some of these courts relied on the legislative history to show that Congress agreed not to add electronic communication to the statutory exclusionary rule, but instead added 18 U.S.C. § 2518(10)(c), which provided for suppression of electronic communications only under the judicially created exclusionary rule.⁵

⁴ The Government also argues that omitting the identity of the authorizing DOJ official from an order as it applies to the interception of electronic communications cannot lead to suppression under § 2518(10)(a). The Government cites to § 2516 for support, which provides that:

Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.

18 U.S.C. § 2516(3) (emphasis added). The Government claims that because the Wiretap Orders reference applications that were made by a Special Assistant U.S. Attorney, who is authorized under § 2516 as “any attorney for the Government,” the Wiretap Orders are not required to state the name of the DOJ official authorizing the interception as it pertains to electronic communications.

⁵ *See* Senate Report No. 99-541, 103 Cong., 2d Sess., 1986 U.S. Code Cong. & Ad. News 3577; *see also* Michael S. Leib, *E-Mail and the Wiretap Laws: Why Congress Should Add Electronic Communication to Title III's Statutory Exclusionary Rule and Expressly Reject a “Good Faith” Exception*, 34 HARV. J. ON LEGIS. 393 (1997).

However, the Fifth Circuit briefly addressed this issue in 1992 when it stated, without explanation, that the Title III exclusionary rule applies to all three types of communication: wire, oral, and electronic. *United States v. Smith*, 978 F.2d 171, 175 (5th Cir. 1992) (“this exclusionary rule only applies to communication that is ‘wire,’ ‘oral,’ or ‘electronic’”) (internal citations omitted).

Nevertheless, the undersigned does not need to resolve this issue. The Defendants have not moved to suppress any electronic communications, nor does the evidence establish that the Defendants had any electronic communications intercepted by authority of the Wiretap Orders.

IV. Motion to Suppress

The Defendants move to suppress all fruits of the interception of wire communications on the grounds enumerated in paragraph (ii)—that the Wiretap Orders are *facially insufficient* because they fail to identify the high-level DOJ official who approved the wiretap applications as required by 18 U.S.C. § 2518(4)(d). (Doc. No. 172, p. 9.)

The Government does not dispute that the orders are silent as to which duly authorized DOJ official authorized the application. Instead of explicitly naming the DOJ individual who authorized the request, the orders state that the applications “were authorized by a duly designated official of the Criminal Division, United States Department of Justice pursuant to the power delegated to that official by special designation of the Attorney General of the United States under the authority vested in him by 18 U.S.C. § 2516 . . .” The Government argues that the Defendants’ motion should be denied on five grounds: (1) Defendants lack standing⁶, (2) the Title III Orders

Section 2518(10)(c) reads: “The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.” § 2518(10)(c).

⁶ This challenge was addressed in Section III, discussed *supra*.

are facially sufficient when viewed with the accompanying Applications, (3) any defect is technical and does not warrant suppression, (4) Title III does not allow statutory suppression of intercepted electronic communications such as text messages⁷, and (5) agents relied on the Wiretap Orders in good faith and therefore Title III's exclusionary rule does not apply. (Doc. No. 181, p. 1.)

V. Legal Authority

Since Title III was adopted in 1968, the Supreme Court has addressed the sufficiency of wiretap orders in three landmark cases.

A. United States v. Giordano, 416 U.S. 505 (1974)

In *United States v. Giordano*, the Supreme Court considered which DOJ officials could authorize wiretap applications under Title III, and whether suppression was required when an order was not properly authorized. At the time, the statute limited authority to “[t]he Attorney General, or any Assistant Attorney General specially designated by the Attorney General.” *Id.* at 513. The order stated that the wiretap application was authorized by a specially designated Assistant Attorney General, but this was incorrect—the Executive Assistant to the Attorney General authorized the application. *Id.* at 509–10. The court found that, despite the confusion, there was no facial insufficiency, as “the order, on its face, clearly, though erroneously, identified [the Assistant Attorney General] as the Justice Department officer authorizing the application, pursuant to special designation by the Attorney General. As it stood, the intercept order was facially sufficient under § 2516(1).” *Id.* at 525 n. 14. Accordingly, the wiretap evidence was not suppressed under § 2518(10)(a)(ii).

⁷ This challenge was also addressed in Section III, discussed *supra*.

The Court held that the communications were nevertheless “unlawfully intercepted,” and thus subject to suppression pursuant to section 2518(10)(a)(i), because the Executive Assistant to the Attorney General, who had actually approved the application, lacked statutory authority to do so. In deciding that suppression was appropriate, the Court noted that “Congress intended to require suppression where there is failure to satisfy any of those statutory requirements that directly and substantially implement the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device.” *Id.* at 527. Applying this test, the court was “confident that the provision for pre-application approval was intended to play a central role in the statutory scheme and that suppression must follow when it is shown that this statutory requirement has been ignored.” *Id.* at 528.

In subsequent decisions, courts would interpret *Giordano* as holding that not *every* failure to comply with a provision of the wiretap statute renders the interception unlawful, but that suppression is required only if the statutory provision is one “that directly and substantially implement[s] the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device.” *United States v. Lawson*, 545 F.2d 557, 562 (7th Cir. 1975). This became known as the “core concerns” test—where suppression hinged on whether the alleged violation implicated Congress’ “core concerns” in implementing the protections enumerated in Title III.

B. *United States v. Chavez*, 416 U.S. 562 (1974)

United States v. Chavez, decided the same day as *Giordano*, involved a wiretap application and order that incorrectly identified an Assistant Attorney General as the authorizing official when the authorization had actually come from the Attorney General himself. *Id.* at 565 (*cf. Giordano* at 509-510, whose authorizing agent lacked statutory power to authorize the wiretap order). The

Supreme Court found that the mistake did not render the wiretap order facially insufficient because the Attorney General—an official who possessed statutory authority—had in fact authorized the application. The Court concluded that mere *misidentification* of the official authorizing the application did not make the application unlawfully intercepted within the meaning of § 2518(10)(a)(i) because that identification requirement did not play a “substantive role” in the regulatory system. *Chavez*, 416 U.S. at 578. *Chavez* differed from *Giordano* because in *Giordano*, the alleged insufficiency was that the authorizing DOJ official lacked statutory authority, and in *Chavez*, the insufficiency was based on a mistake. Ultimately, the court in *Chavez* found that the evidence was not subject to suppression for being “unlawfully intercepted” under section 2518(10)(a)(i):

Failure to correctly report the identity of the person authorizing the application . . . when in fact the Attorney General has given the required preliminary approval to submit the application, does not represent a similar failure to follow Title III’s precautions against the unwarranted use of wiretapping or electronic surveillance and does not warrant the suppression of evidence gathered pursuant to a court order resting upon the application.

Id. at 571. Both *Giordano* and *Chavez* focus on paragraph (i), which pertains to allegations that the electronic communication was unlawfully intercepted. Under *Giordano* and *Chavez*, a wiretap order can list an incorrect source of DOJ authority without creating a facial insufficiency, provided that the source listed is statutorily empowered to exercise authority. *United States v. Callum*, 410 F.3d 571, 576 (9th Cir. 2005).

C. *Dahda v. United States*, 138 S. Ct. 1491 (2018)⁸

In *Dahda*, the Supreme Court considered wiretap orders that impermissibly authorized wiretaps outside the District of Kansas, where the orders had been issued. The defendants claimed that the evidence obtained should be suppressed because the language in the order that purported to authorize wiretaps outside the District of Kansas made the order “insufficient on its face” within the meaning of § 2518(10)(a)(ii). *Id.* at 1493.

The Tenth Circuit applied the *Giordano* “core concerns” test to hold that paragraph (ii) applies only where the insufficiency reflects an order’s failure to satisfy the “statutory requirements that directly and substantially implement the congressional intention to limit the use of” wiretapping. *Dahda*, 138 S. Ct. at 1493. The court identified two core concerns, concluded that neither applies to the surplusage included on the order that extended the territorial limitation, and denied the defendant’s motion to suppress. *Id.*

The Supreme Court rejected the Tenth Circuit’s reasoning, and held that the *Giordano* “core concerns” test does not apply to paragraph (ii) challenges:

The underlying point of *Giordano*’s limitation was to help give independent meaning to each of § 2518(10)(a)’s paragraphs. It thus makes little sense to extend the core concerns test to paragraph (ii) as well. Doing so would “actually treat that paragraph as ‘surplusage’—precisely what [this] Court tried to avoid in *Giordano*.” We consequently conclude that paragraph (ii) does not contain a *Giordano*-like “core concerns” requirement. The statute means what it says. That is to say, paragraph (ii) applies where an order is “insufficient on its face.”

⁸ It is important to note that from the *Giordano* and *Chavez* decisions in 1974 until *Dahda* was decided in 2018, multiple Circuit and District Courts examined these issues with varying results. *See, e.g., United States v. Small*, 423 F.3d 1164, 1178 (10th Cir. 2005) (holding that a wiretap order’s failure to identify the person authorizing the application does not require suppression of the wiretap evidence, where the wiretap application was authorized by an appropriate individual within the Department of Justice and that authorizing individual was identified by name in the wiretap application); *United States v. Radcliff*, 331 F.3d 1153, 1160 (10th Cir. 2003) (same); *United States v. Guzman-Torres*, No. CR-11-0234-HE, 2011 WL 4639922, at *2 (W.D. Okla. Oct. 4, 2011) (same); *United States v. Fudge*, No. 01-CR-09-C-5, 2001 WL 34377928, at *6–7 (W.D. Wis. Jun. 21, 2001) (same); *but see United States v. Scurry*, 821 F.3d 1 (D.C. Cir. 2016) (holding that Title III mandates suppression where wiretap authorization orders were facially insufficient for failure to specify the identities of the individual high-level Justice Department officials who authorized the wiretap applications).

Dahda, 138 S. Ct. at 1498 (internal citations omitted). The Court also referenced the Oxford English Dictionary for guidance in determining insufficiency: insufficient means “deficient” or “lacking in what is necessary or requisite.” *Id.* (citing *Oxford English Dictionary* 359 (1933)). However, the Court was careful to restrict the veil of protection offered by paragraph (ii) in clarifying that not *any* legal defect that appears within the four corners of an order compels a finding of insufficiency and compels suppression. Instead, the Court reasoned that—at a *minimum*—the information required by § 2518(4) is required, and if lacking, would render an order “insufficient on its face.” *Id.* at 1498; (referring to §§ 2518(4)(a)–(e) (requiring an order to specify, *inter alia*, the identity of the person authorizing the application)).

VI. Discussion

The issue before the court is whether the Wiretap Orders are facially insufficient for failing to identify the authorizing DOJ official, and if so, whether this insufficiency warrants suppression. This issue has been a matter of dispute in various courts for decades and has resulted in different rulings. However, now that the Supreme Court has made clear that the “core concerns” test does not apply to facial insufficiency challenges under § 2518(10)(a)(ii), the undersigned finds that suppression should be granted.

The Defendants rely on *Giordano* and *Chavez* to support their argument that the court must examine the four corners of the order and establish whether, on its face, the § 2518(4) requirements are satisfied. (Doc 172., p. 3.) The Defendants also rely on a case from the Court of Appeals for the D.C. Circuit, *United States v. Scurry*, 821 F.3d 1 (D.C. Cir. 2016). In *Scurry*, like here, the wiretap order did not include the identity of the high-level DOJ official who authorized the wiretap application.⁹ *Id.* at 367. The D.C. Circuit Court examined the four corners of the order as required

⁹ Instead of listing an actual name of a person with authority, the *Scurry* orders had asterisks where presumably the name should have been noted.

by *Chavez* and *Giordano* to find the order to be insufficient on its face: “There can be little question that each of the [Defendants’] orders is ‘insufficient on its face’ . . . because each fails to include information expressly required by Title III.” *Id.* at 8 (internal citations omitted). Given that the orders authorizing the wiretaps in *Scurry* did not specify the statutorily required high-ranking DOJ official who had signed off on the underlying application, the D.C. Circuit mandated that the information collected pursuant to the wiretaps be suppressed. *Id.* (“To determine whether a wiretap order is facially insufficient, a reviewing court must examine the four corners of the order and establish whether, on its face, it contains all that Title III requires it to contain.”) (noting that the D.C. Circuit’s previous opinion in *United States v. Glover*, 736 F.3d 509, 515 (D.C. Cir. 2013), “left open the possibility that a ‘technical defect’ in a wiretap order might not rise to the level of facial insufficiency, but rather would render the order ‘imperfect’”).

In response, the Government relies on *Chavez* to argue that “not every failure to comply fully with any requirement provided in Title III” warrants suppression. The Government claims that the *application* identifies the authorizing individual, and that the order references the application—so by extension—the § 2518(4) requirements are satisfied.¹⁰ The Government recognizes the recent ruling in *Dahda*—that the Supreme Court has rejected the “core concerns”

¹⁰ The first sentence of the Wiretap Orders includes the phrase: “Application under oath having been made to me . . . and full consideration having been given to the matter set forth therein.” The Government argues that this statement establishes that the Wiretap Orders “incorporated the Applications and expressly referred the reviewing judge to those Applications. By signing the [Wiretap] Orders, as every reviewing judge did in this case, the judges committed to having given full consideration [to] the matter set forth ‘therein,’ referring to the Application and its attachments.” (Doc. 181, p. 9-10.)

However, each identification requirement has a distinct audience in the Title III process. *Scurry*, 821 F.3d at 11. “Requiring identification of the authorizing official in the *application* facilitates the court’s ability to conclude that the application has been properly approved under § 2516. . . .” *Chavez*, 416 U.S. at 575 (emphasis added). “Including that identification in the wiretap *order* facilitates additional oversight, this time by the parties executing the order.” *Scurry*, 821 F.3d at 11 (emphasis added).

In any event, despite the Government’s argument to the contrary, there is no language in the Wiretap Order that explicitly incorporates by reference the applications and exhibits. The introductory phrase relied on by the Government is nothing more than a simple acknowledgement that the issuing judge considered the application, as required by law.

approach for paragraph (ii) insufficiencies—but argues that because the *applications* contain the required name of the authorizing person, the insufficiency on the order itself constitutes a technical defect, which under *Dahda* does not require suppression. The Government also relies on a series of pre-*Dahda* circuit cases that have denied suppression under similar facts. See *United States v. Radcliff*, 331 F.3d 1153, 1163 (10th Cir. 2003) (holding that failure to identify authorizing person in order constitutes technical defect); and *United States v. Traitz*, 871 F.2d 368, 379 (3d Cir. 1989) (holding that the purpose of § 2518(4)(d) was not undermined where the authorizing official was named in the wiretap application but not in the wiretap order).

However, the Government’s reliance on any pre-*Dahda* case is outdated. Prior to *Dahda*, many courts applied the “core concerns” test when analyzing whether a wiretap order was sufficient on its face. See *Traitz*, 871 F.2d at 379; *United States v. Vigi*, 515 F.2d 290, 293 (6th Cir. 1975). Again, the Supreme Court in *Dahda* made clear that the core concerns test does not apply to paragraph (ii) challenges, and narrowly defined what constitutes “facial insufficiency”:

It is clear that paragraph (ii) covers at least an order’s failure to include information that § 2518(4) specifically requires the order to contain. See §§ 2518(4)(a)–(e) (requiring an order to specify, *e.g.*, the “identity of the person, if known, whose communications are to be intercepted,” “a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates”). **An order lacking that information would deviate from the uniform authorizing requirements that Congress explicitly set forth, while also falling literally within the phrase “insufficient on its face.”**

Dahda, 138 S. Ct. at 1498 (internal citations omitted) (emphasis added).

Section 2815(4) requires that the *order*—not the application—contain the “identity . . . of the person authorizing the application.” 18 U.S.C. § 2815(4)(d). The Wiretap Orders at issue do not contain this information. Instead, the Wiretap Orders provide a troublingly vague reference to a “duly designated official of the Criminal Division, United States Department of Justice pursuant to the power delegated to that official by special designation of the Attorney General of the United

States under the authority vest in him by Section 2516 . . .” This description casts a wide net and does not narrowly identify the person authorizing the application.

Although Congress has amended Title III since its enactment in 1968, Congress has not changed the information required in a wiretap court order. *Compare* 18 U.S.C. § 2518(4)(a)–(e), with Title III, § 802, 82 Stat. at 219 (adding section 2518(4)(a)–(e) to Title 18). As the Supreme Court observed in *Chavez*, “[t]here is little question that [the identification requirements] were intended to make clear who bore the responsibility for approval of the submission of a particular wiretap application.” *Chavez*, 416 U.S. at 571-72. “To specify a category of official or a job title is usually not the same thing as specifying the ‘identity’ of a ‘person.’” *Scurry*, 821 F.3d at 11. The § 2518(4)(d) requirement that a wiretap order identify the person who authorized the wiretap application exists so that “[s]hould abuses occur, the lines of responsibility [would] lead to an *identifiable person*.” *Scurry*, 821 F.3d at 11 (citing S. REP. NO. 90–1097, at 197) (emphasis added).

The undersigned cannot reconcile how the Wiretap Orders—and their blatant failure to comply with the § 2518(4)(d) requirement to identify the person authorizing the application—can satisfy scrutiny for facial insufficiency in a post-*Dahda* regime. Although the Government urges the court to see this glaring deficiency as a mere “technical defect,” the Supreme Court is clear that any failure to include information required by the § 2518(4) requirements renders the order facially insufficient under paragraph (ii). *Dahda*, 138 S. Ct. at 1498. As the Supreme Court also recognized, “[t]he statute means what it says.” *Id.*; *see also New Orleans Depot Servs., Inc. v. Dir., Office of Worker’s Comp. Programs*, 718 F.3d 384, 393 (5th Cir. 2013) (en banc) (“[T]he first rule of statutory construction is that we may not ignore the plain language of a statute.”). The statute very clearly states that the *order* must contain the identity of the person authorizing the

application. A reference to a “duly appointed” DOJ official—with no other identifying title or name—falls woefully short of creating a trail of responsibility to an *identifiable person*. Accordingly, the Wiretap Orders are insufficient on their face, and the evidence derived therefrom should be suppressed.

VII. The Government’s Good Faith Defense

The Government claims that the Wiretap Orders were obtained well before *Scurry* and *Dahda* were decided, and that the court should be bound by the legal authority as it existed at the time the orders were signed. The Government cites to the Supreme Court’s holding in *Davis v. United States*, 564 U.S. 229, 241 (2011), which held that evidence obtained during a vehicle search conducted in reasonable reliance on binding precedent is not subject to the exclusionary rule. While neither the Supreme Court nor the Fifth Circuit has addressed whether the good faith exception applies to suppression claims brought under § 2518, this issue has been litigated at the circuit level with varying results.¹¹ The Sixth Circuit and the D.C. Circuit have concluded that the good faith exception is inapplicable to Title III wiretap cases. *See United States v. Rice*, 478 F.3d 704, 711-14 (6th Cir. 2007) and *United States v. Glover*, 736 F.3d 509, 513 (D.C. Cir. 2013), *abrogated by Dahda*. Whereas the Fourth, Eighth, and Eleventh Circuits have held that it does apply. *See United States v. Moore*, 41 F.3d 370, 376 (8th Cir. 1994); *United States v. Malekzadeh*, 855 F.2d 1492, 1497 (11th Cir. 1988); *see also United States v. Brewer*, 204 F. App’x 205, 208 (4th Cir. 2006) (unpublished).

The undersigned finds no need to analyze whether the good faith exception applies to Title III cases. Because even if it does, the Government does not prove, nor does the evidence establish,

¹¹ The issue was also addressed in the Eastern District of Louisiana, which held that the “good faith” exception to the exclusionary rule does apply in Title III cases. *United States v. Davis*, No. CR.A. 01-282, 2003 WL 548910, at *10 (E.D. La. Feb. 25, 2003).

that the Government's error was the result of "reasonable reliance" on binding precedent. At the time the Wiretap Orders were executed in 2014, there was no binding Fifth Circuit or Supreme Court case holding that evidence obtained from a facially insufficient wiretap order should not be suppressed as long as the "core concerns" test is satisfied. In fact, the Supreme Court in *Dahda* recognized that *Giordano* was trying to avoid having "core concerns" test apply in facial sufficiency challenges. *Dahda*, 138 S. Ct. at 1498 (holding that the underlying point of *Giordano*'s limitation was to help give independent meaning to each of § 2518(10)(a)'s paragraphs, and that it makes little sense to extend the core concerns test to paragraph (ii) as well).

The § 2815(4) requirements are remarkably clear—wiretap orders must contain the identity of the person authorizing the application. The statute means what it says, and any assumption otherwise is simply not reasonable nor deserving of the good faith exception. Moreover, it is worth noting that the issue of facial sufficiency of wiretap orders is not a novel concept—this issue has been litigated since the 1970's. Nearly every circuit and many district courts have addressed the sufficiency of wiretap orders, with some involving analogous facts to this case. And yet, many of the same deficiencies or issues keep occurring, requiring court intervention, and in some instances, suppression is the result. In an effort to avoid matters of contention and possible suppression, the Department of Justice and its officers should be reminded that "Title III is an exacting statute obviously meant to be followed punctiliously." *Callum*, 410 F.3d at 579. The *orders*—not just the applications—require the five elements listed in § 2518(4), including the identity of the person authorizing the application. One would plausibly think this requirement could very easily be satisfied by listing the actual name of the authorizing official in the order itself. This is a very simple step in the complicated process of preparing the application and order, and yet it seems to oftentimes be overlooked or forgotten.

VIII. Recommendation

Title III requires that wiretap orders specify the identity of any person authorized to make the wiretap application. 18 U.S.C. § 2518(4)(d). The Government concedes that the Wiretap Orders in this case do not provide this necessary element. The undersigned finds that this deficiency renders the Wiretap Orders facially insufficient. Because an aggrieved person may move to suppress the contents of wire communications intercepted or the evidence derived therefrom on the grounds that the wiretap order is insufficient on its face, the undersigned recommends granting the Defendants' Motion to Suppress.

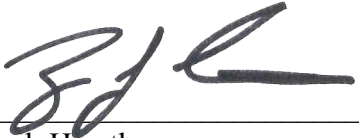
IX. Objections

Pursuant to 28 U.S.C. § 636(b)(1)(c), each party to this action has the right to file objections to this report and recommendation. Objections to this report must: (1) be in writing, (2) specifically identify those findings or recommendations to which the party objects, and (3) be served and filed within fourteen (14) days after being served with a copy of this report, and (4) no more than eight (8) pages in length. *See* 28 U.S.C. § 636(b)(1)(c) (2009); FED. R. CIV. P. 72(b)(2); Local Rule CV-72(c). A party who objects to this report is entitled to a *de novo* determination by the United States District Judge of those proposed findings and recommendations to which a specific objection is timely made. *See* 28 U.S.C. § 636(b)(1) (2009); FED R. CIV. P. 72(b)(3).

A party's failure to file specific, written objections to the proposed findings of fact and conclusions of law contained in this report, within fourteen (14) days of being served with a copy of this report, bars that party from: (1) entitlement to *de novo* review by the United States District Judge of the findings of fact and conclusions of law, *see Rodriguez v. Bowen*, 857 F.2d 275, 276–77 (5th Cir. 1988), and (2) appellate review, except on grounds of plain error, of any such findings

of fact and conclusions of law accepted by the United States District Judge, *see Douglass v. United Servs. Auto. Ass'n*, 79 F.3d 1415, 1428–29 (5th Cir. 1996) (en banc).

SIGNED this 2nd day of November, 2018.



Zack Hawthorn
United States Magistrate Judge